CLAIMS:

1. Processor for encrypting and/or decrypting data, wherein a control device (12) is connected to at least one encryption/decryption means (14) via at least one communication means (16), the control device (12) is connected to at least one rounding key generation means (18) via at least one further communication means (20), the control device (12) has at least one external key input (22), the at least one encryption/decryption means (14) has at least one external data input (24) and at least one external data output (26), and the at least one encryption/decryption means (14) and the at least one rounding key generation means (18) are decoupled from one another.

2. A processor as claimed in claim 1, characterized in that the at least one communication means (16) comprises at least one request line, at least one release line and at least one data line and/or the at least one further communication means (20) comprises at least one further request line, at least one further release line and at least one further data line.

3. A processor as claimed in any of the preceding claims, characterized in that the at least one request line, the at least one release line and the at least one data line and/or the at least one further request line, the at least one further release line and the at least one further data line at least partially use the same line physics.

4. A processor as claimed in any of the preceding claims, characterized in that the control device (12) comprises at least one storage means (28) in which at least one rounding key generated by the at least one rounding key generation means (18) can be temporarily stored.

5. A processor as claimed in claim 4, characterized in that at least one rotating pointer is provided for access to the at least one storage means (28).

6. A processor as claimed in any of the preceding claims, characterized in that at least one handshake protocol is provided for communication of the control device (12) with

the at least one encryption/decryption means (14) and/or with the at least one rounding key generation means (18).

7. A processor as claimed in any of the preceding claims, characterized in that the modes of operation of the control device (12), of the at least one encryption/decryption means (14) and of the at least one rounding key generation means (18) are asynchronous with respect to one another.

8. A processor as claimed in any of the preceding claims, characterized in that at least one dummy calculation and/or at least part of at least one previous rounding key calculation can be carried out by means of the at least one rounding key generation means (18) during at least one inactive phase.

9. A processor as claimed in any of the preceding claims, characterized in that the time between calculation and use of the at least one rounding key is variable.

10. A processor as claimed in any of the preceding claims, characterized in that said processor is embodied so as to be an AES coprocessor.

11. A method of encrypting and/or decrypting data using a processor as claimed in at least one of claims 1 to 9, wherein

a) at least one initial key is read into a control device,

b) external data are read into at least one encryption/decryption means,

c) at least one data word needed to calculate at least one rounding key is read from at least one storage means of the control device and transferred to at least one rounding key generation means,

d) at least one rounding key is calculated recursively on the basis of the at least one data word by means of the at least one rounding key generation means, transferred to the control device and stored in the at least one storage means,

e) the at least one rounding key is transferred to the at least one encryption/decryption means,

f) the external data are encrypted or decrypted by means of the at least one encryption/decryption means using the at least one rounding key and the encrypted or decrypted data are made available at at least one external data output, and

g) steps b) to f) are repeated as often as necessary to encrypt or decrypt a set of external data.

12. A method as claimed in claim 11, characterized in that the communication of the control device with the at least one encryption/decryption means and/or the at least one rounding key generation means takes place by means of at least one handshake protocol.

13. A method as claimed in either of claims 11 and 12, characterized in that the communication of the control device with the at least one encryption/decryption means and the at least one rounding key generation means takes place asynchronously.

14. A method as claimed in any of claims 11 to 13, characterized in that access to the at least one storage means takes place by means of at least one rotating pointer.

15. A method as claimed in any of claims 11 to 14, characterized in that at least one dummy calculation and/or at least part of at least one previous rounding key calculation is carried out by means of the at least one rounding key generation means during at least one inactive phase.

16. A method as claimed in any of claims 11 to 15, characterized in that the time between calculation and use of the at least one rounding key is variable.

17. A method as claimed in any of claims 10 to 16, characterized in that it is embodied as a method of AES calculation using an AES coprocessor as claimed in claim 10.